WiNG 5.X How-To Guide

Smart RF

Part No. TME-04-2014-04 Rev. B

Table of Contents

1. Overview

Self Monitoring At Run Time RF Management (Smart RF) is a Motorola Solutions innovation designed to simplify RF configurations for new deployments, while providing on-going optimization as the RF environment changes over time.

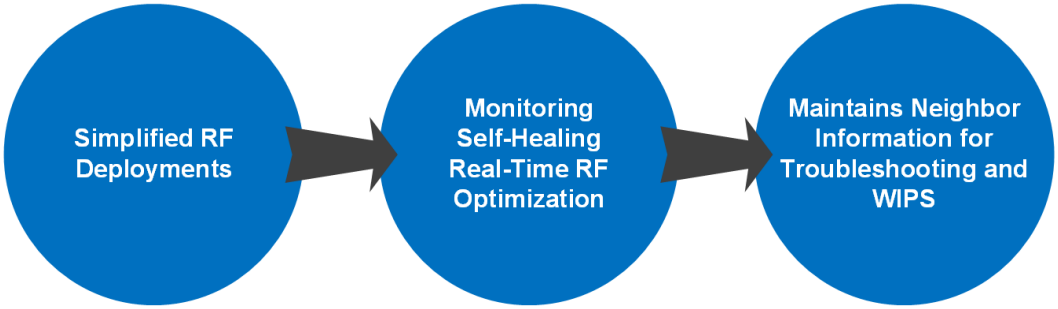


Figure 1 – Smart RF Benefits

Smart RF can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power for each Smart RF managed radio. Smart RF policies can be added to specific RF Domains to apply site specific deployment configurations and self-healing values to groups of Access Points (APs).

Smart RF distributes the decision process between RF Domain Managers which make intelligent RF configuration decisions using data obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs by constantly monitoring the RF environment for external Wi-Fi interference, neighbor Wi-Fi interference, non-Wi-Fi interference and client connectivity. Smart RF then intelligently applies various algorithms to arrive at the optimal channel and power selection for all APs in the network and constantly reacts to changes in the RF environment.

Smart RF is supported in WiNG 5.0 and above on all RF Switches, Network Services Platforms and 802.11n/ac Access Points for all deployment models.

Figure 1-2 – Supported Access Points

Note: Off-Channel Scanning (OCS) is only supported on the 2.4 GHz and Sensor radio on the AP 82XX series Access Points. OCS is not currently supported on the 802.11ac radio.

1.1 Off-Channel Scanning

Smart RF leverages the Off-Channel-Scanning (OCS) capabilities built into each Motorola Solutions 802.11n/ac Access Point (AP) to monitor the RF environment in real-time on both 2.4 GHz and 5 GHz bands. When Smart RF is enabled in WiNG 5, each Smart RF managed radio by default will go off-channel for 50 milliseconds every 6 seconds (configurable) to monitor the RF environment for each channel. Over time each radio is able to gain a full picture of the RF environment and learn:

1. Neighboring APs
2. Sources of Wi-Fi Interference
3. Sources of Non-Wi-Fi Interference

The RF environmental information is collected by each AP and forwarded to the elected RF Domain Manager for the RF Domain who co-ordinates the channel and power decisions. The RF environmental information is also used by Smart RF to make intelligent power and channel changes as the RF environment evolves over time as well as initiate Neighbor Recovery, Interference Recovery and Coverage Hole Recovery features.

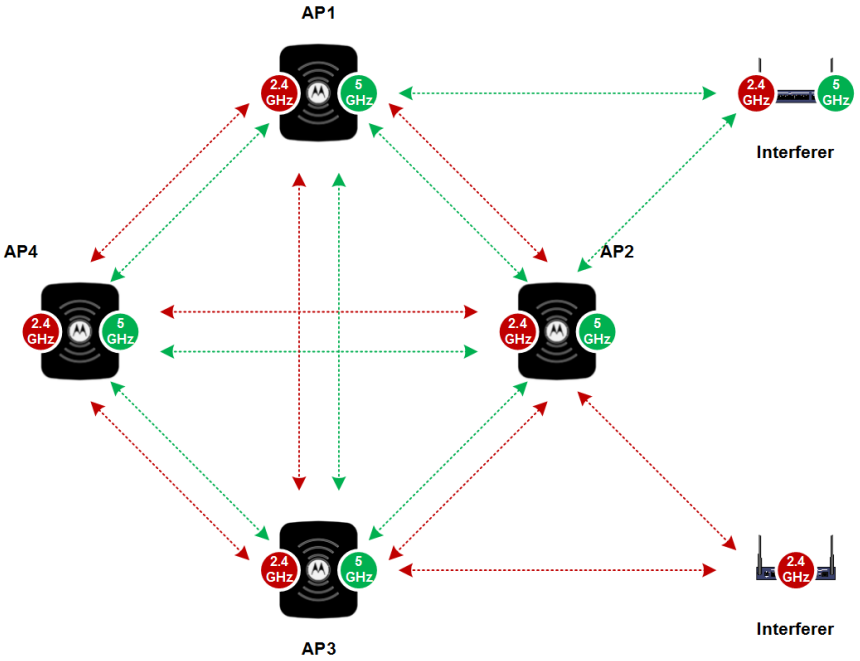


Figure 1.1 – Off-Channel Scanning

OCS is also leveraged by other WiNG 5 features such as Basic WIPS and Enhanced Base WIPS to determine if unsanctioned or rogue Access Points are present at a site. Each detected Interfering device is added to the AP Detection table allowing administrators to view all the non-managed APs that are visible at each site. The Base Enhanced WIPS feature can additionally detect if an Interfering AP is present on the wired network (i.e. classified as a rogue) and automatically initiate air terminations to mitigate the rogue.

Note: The Enhanced Base WIPS feature is included as part of the WiNG 5.6 release and depreciates the Basic and Advanced WIPS features from previous WiNG 5 releases.

1.2 Channel and Power Selection

The channels and power values assigned to the Smart RF managed radios are dependent on the country code assigned to the RF Domain, the channel and power configuration defined in the Smart RF Policy / RF Domain and if the Smart RF Policy is enabled:

1. If the Smart RF Policy assigned to the RF Domain is enabled, the channel and power assigned to each Smart RF managed radio is based on the channel and power values defined within the Smart RF Policy. The channel and power values are intelligently selected based on the neighbor AP placement and interfering devices.
2. If the Smart RF Policy assigned to the RF Domain is disabled, the assigned channels are randomly selected from the channel list defined within the Smart RF Policy. The assigned channels persistent until the AP is rebooted or the radios are disabled / re-enabled. The power of each radio is set to the highest permissible value.
3. If no Smart RF Policy is assigned to the RF Domain, Auto Channel Selection (ACS) is used for channel assignment where each radio is assigned a channel with the least interference possible. Radios wait 20 – 30 seconds before starting ACS to avoid multiple radios going to the same channel.

Each channel and power parameter is fully configurable within the Smart RF Policy allowing an administrator to tweak the system to suite their specific Wi-Fi deployment needs. For example administrators can modify the Smart RF policy to exclude DFS channels or lower the minimum / maximum power values for high-density deployments. By default Smart RF will assign radios a power value between 4 dBm to 17 dBm, a 20 MHz channel to each 2.4 GHz radio and a 40 MHz channel to each 5 GHz radio.

Parameter	2.4 GHz Radio Defaults	5 GHz Radio Defaults
Min Power	4 dBm	4 dbm
Max Power	17 dBm	17 dBm
Channel Width	20 GHz	40 GHz
Channels	1,6,11	21, 25, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165, 173

Table 1.2 – Smart RF Channel & Power Defaults

Certain 5 GHz channels are subject to FCC / ETSI Dynamic Frequency Selection (DFS) regulations. If a Smart RF enabled radio is on a channel subject to DFS, it will switch channels if radar is detected on the assigned 5 GHz channel. By default the Access Point radio will attempt to come back to its original channel after the DFS channel evacuation period has expired. This can be optionally disabled in the CLI by issuing the ***no dfs-rehome*** command in the radio configuration context in the Access Point Profile.

1.3 Recovery Features

Smart RF supports self-healing features by monitoring the RF environment in real-time and provides automatic mitigation from potentially problematic events such as neighbor interference, non-Wi-Fi interference (noise), external Wi-Fi interference, coverage holes and radio failures. Smart RF employs self-healing to maintain Wi-Fi client performance and Wi-Fi coverage during dynamic RF environment changes, which typically requires manual intervention to resolve.

The Smart RF recovery features are only intended to provide a temporary measure until a permanent fix is applied. For example if a remote site is experiencing constant Coverage Hole Recovery events for Wi-Fi clients within a specific coverage area, the administrator will need to re-survey the area and determine if deploying an additional Access Point (AP) or different antennas can remediate the coverage problem. Likewise if an AP in a coverage area fails or becomes faulty, the administrator will need to replace the failed / faulty AP to permanently remediate the problem.

The only recovery feature in which a permanent fix may not be feasible is Interference Recovery where the interfering APs may not be or owned or managed by the company or division. In this case Smart RF will simply adjust the channels and power values on the Smart RF managed radios to provide the best possible RF environment around the interfering devices.

1.3.1 Interference Recovery

Smart RF provides mitigation from Wi-Fi sources of interference by measuring noise and interference on each Smart RF managed radios current channel. When a noise threshold is exceeded, Smart RF can select an alternative channel for the Smart RF managed radio with less interference. To avoid channel flapping, a hold-timer is defined which disables interference avoidance for a specific period of time upon detection. Interference Recovery is enabled by default.

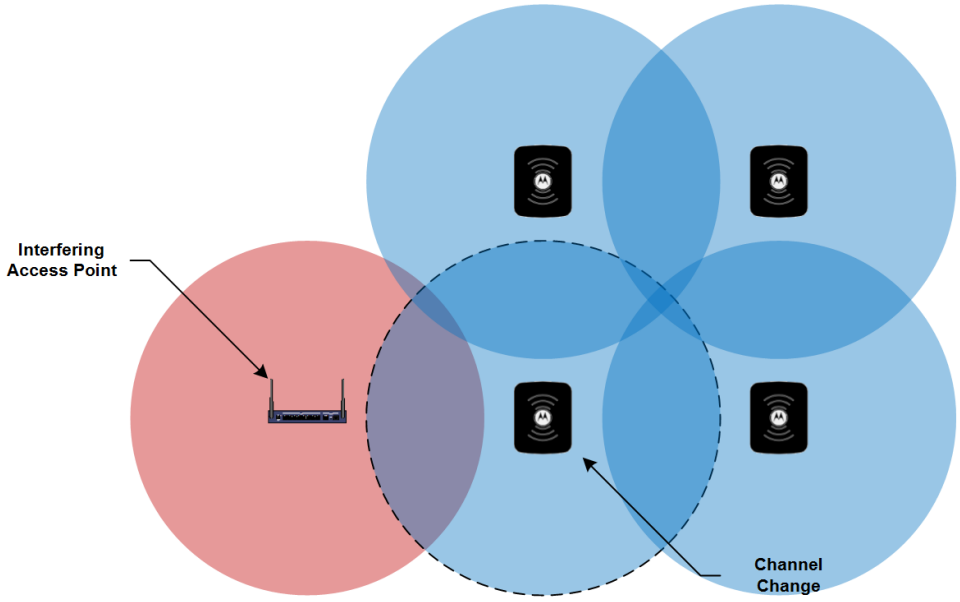


Figure 1.3.1 – Interference Recovery Example

1.3.2 Neighbor Recovery

Smart RF provides automatic recovery for failed or faulty Access Points (APs) or faulty antennas by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. Using Smart RF probes each Smart RF managed radio maintains an active list of neighboring Smart RF managed radios which includes each neighbors channel, power and attenuation. If a neighboring Smart RF radio drops below a defined power threshold, one or more Smart RF managed radios can increase their power to compensate for the coverage loss. Neighbor recovery is enabled by default and requires a minimum of 4 APs to function.

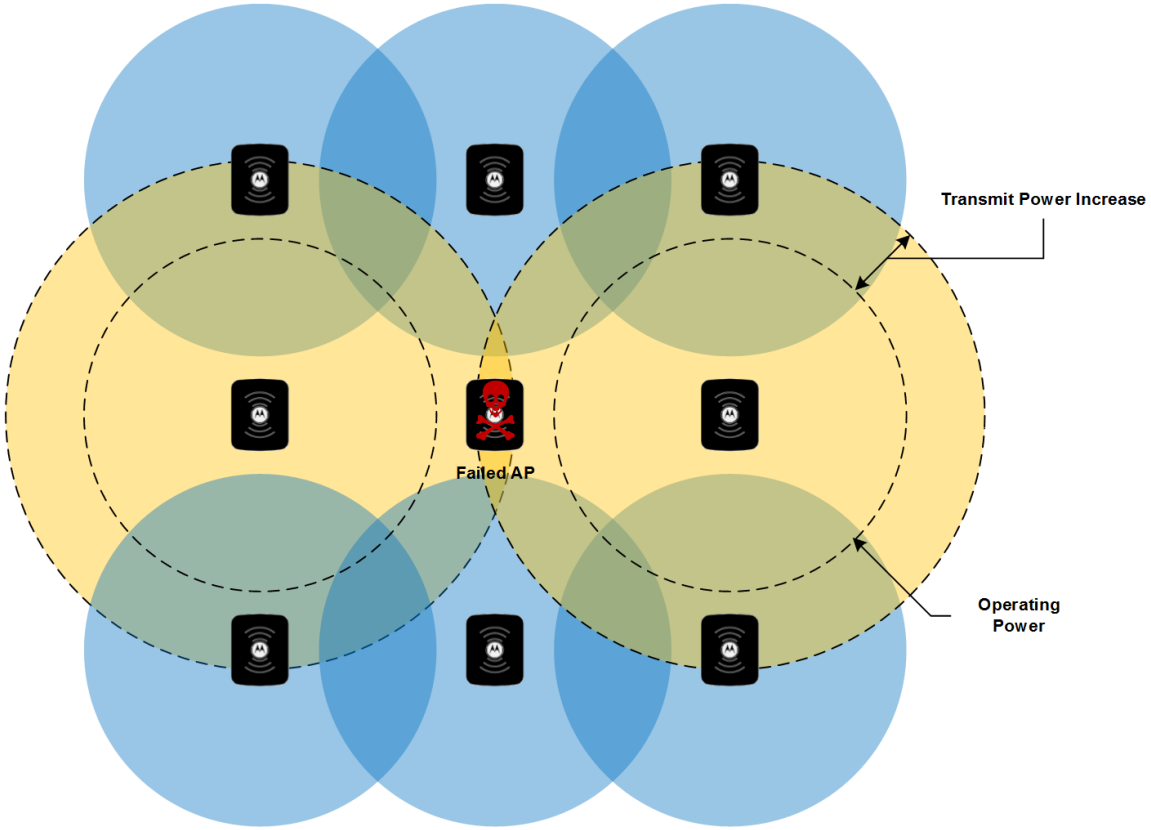


Figure 1.3.2 – Neighbor Recovery Example

Note: A Smart RF managed radio will only change power if a power difference of +/-3 is necessary. The power adjustment can also be >3 for example if a radio is operating at 10 and the Smart RF algorithm determines the power needs to be 17, the Smart RF radio will change to 17 immediately. However power decreases will always occur in steps of 3.

1.3.3 Coverage Hole Recovery

Smart RF provides mitigation for coverage issues for Wi-Fi clients located at the fringes of the network or in poor coverage areas. When coverage hole is detected, Smart RF first determines the power compensation needed based on the signal to noise ratio (SNR) for a client as seen by the Smart RF managed radio. If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. Coverage Hole Recovery is enabled by default.

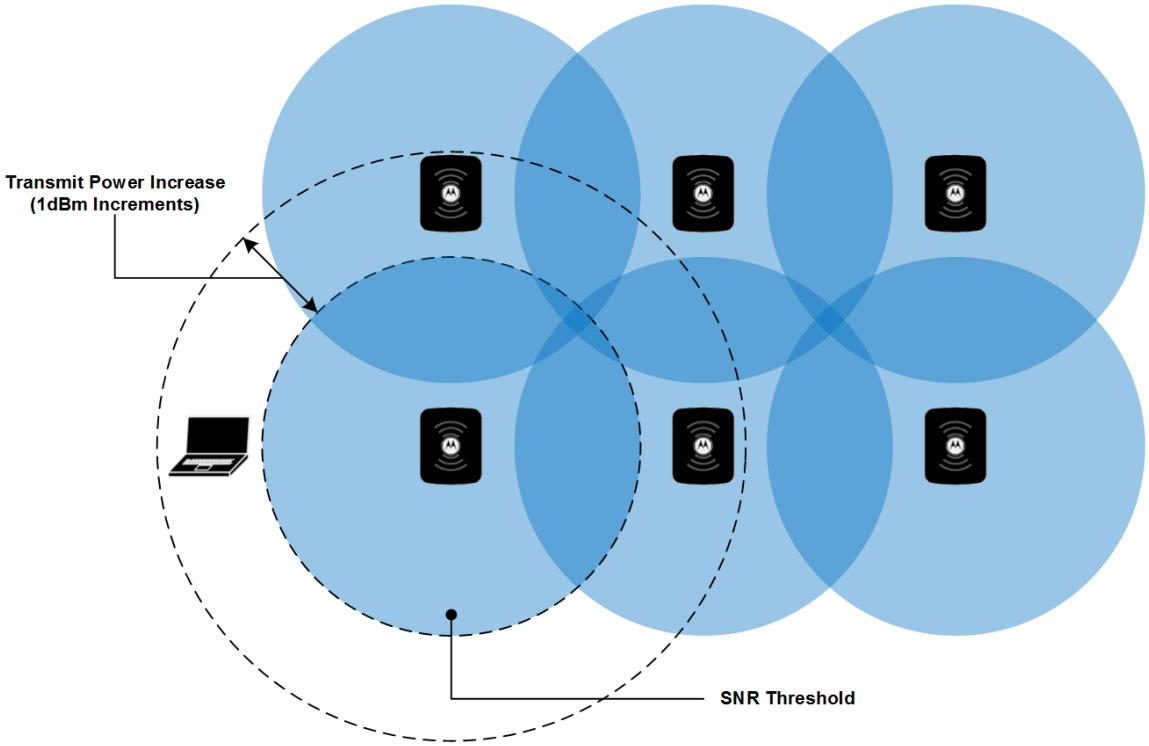


Figure 1.3.3 – Coverage Hole Recovery Example

2. Smart RF Policy

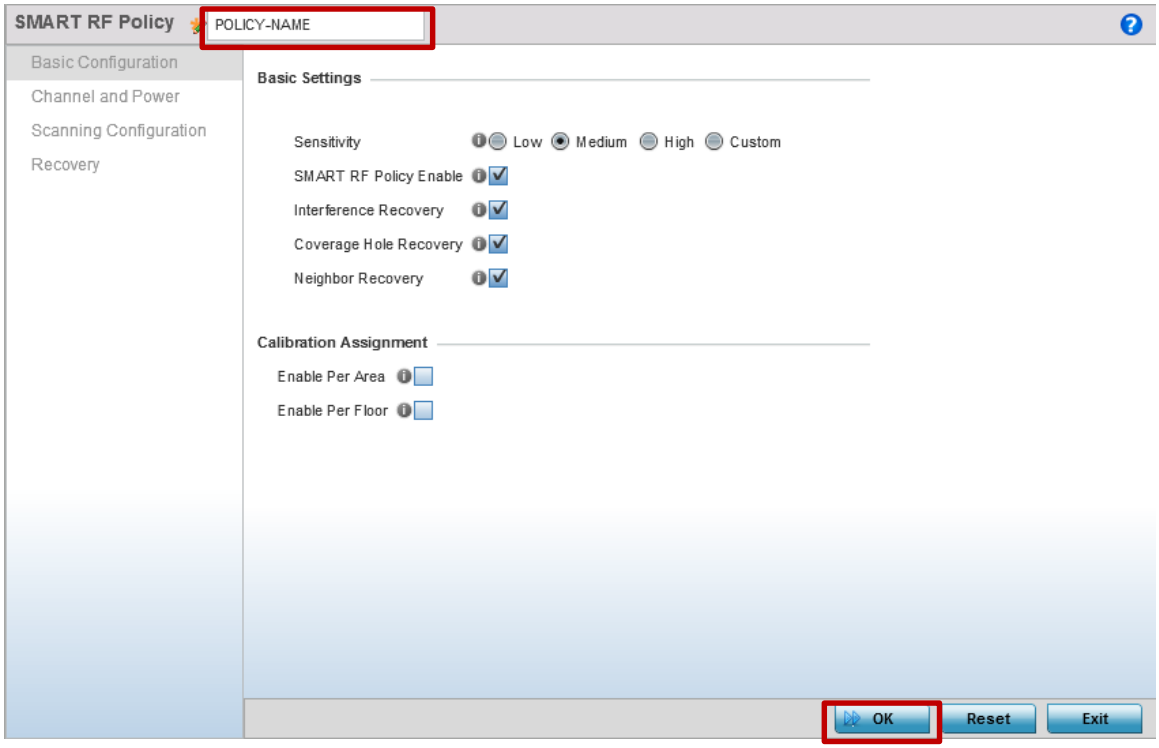
Enabling Smart RF requires that you define a Smart RF Policy which is assigned to one or more RF Domains. By default each default and user defined Access Point (AP) Profile will configure each radio to use Smart RF for both channel and transmit power assignments.

Most WiNG 5 deployments will consist of a common Smart RF Policy which is assigned to each RF Domain in the system, however it is not uncommon for customers to define separate Smart RF Policies for stores, offices and warehouses as APs are deployed differently in each environment and the Wi-Fi clients will have different coverage and density requirements.

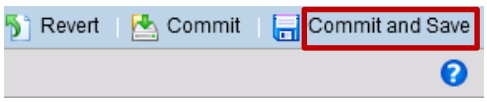
A Smart RF Policy can be created in WiNG 5 using either the CLI or Web-UI. The following procedure describes how to create a new Smart RF Policy using the Web-UI. Note that by default the Smart RF Policy will be assigned a Medium Sensitivity value:

1 **Select *Configuration* → *Wireless* → *SMART RF Policy* then click *New*. Name the new Policy then click *OK*:**

Configuration* → *Wireless* → *SMART RF Policy* → *New



2 **Select *Commit and Save*:**



The following procedure describes how to create a new Smart RF Policy using the CLI. As with the Web-UI, by default the Smart RF Policy will be assigned a Medium Sensitivity:

Enable Privileged Context:

```
RFS4000-1> enable
```

Enter the Configuration Context:

```
RFS4000-1# configure terminal
```

Create a new Smart RF Policy:

```
RFS4000-1(config)# smart-rf-policy <name>
```

Commit and Save the changes:

```
RFS4000-1(config-smart-rf-policy-<name>)# commit write
```

2.1 Basic Configuration

The Basic Configuration screen in the Smart RF Policy includes the following configuration sections:

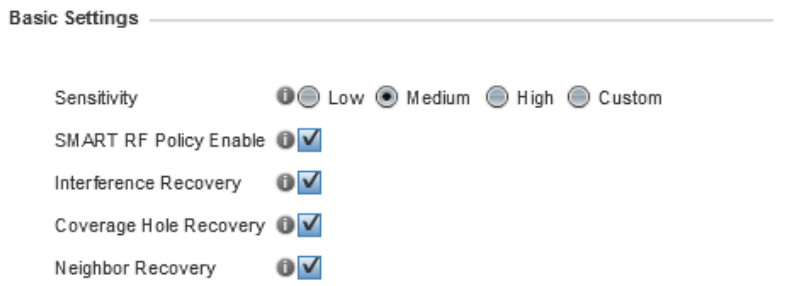
- ***Basic Settings*** – Determines the sensitivity, policy state as well as the Smart RF recovery features that are enabled.
- ***Group By*** – Determines if Smart RF calculations are performed Per Area or Per Floor.

2.1.1 Basic Settings

The Basic Settings parameters are used to determine the Off-Channel Scanning (OCS) aggressiveness used by Smart RF for monitoring and configuration. Changing the Smart RF Sensitivity modifies values in the Scanning Configuration, Neighbor Recovery, Interference Recovery and Coverage Hole Recovery screens. As a general best practice it is recommended that you only use the default Medium Sensitivity which has been proven to work well in retail, office and warehouse environments. If customization is required, it is recommended that the custom values be based on the Medium Sensitivity values.

The additional Basic Settings parameters determine if the Smart RF Policy is enabled and which Recovery features are enabled. The choice as to which Recovery features you enable will be determined by the AP placement and overlapping coverage provided at each site. Note that the Recovery features can only operate correctly if adequate coverage and overlap has been designed into the system.

Web-UI



CLI Command Syntax

```
sensitivity (low|medium|high|custom)
[no] enable
[no] interference-recovery
[no] coverage-hole-recovery
[no] neighbor-recovery
```

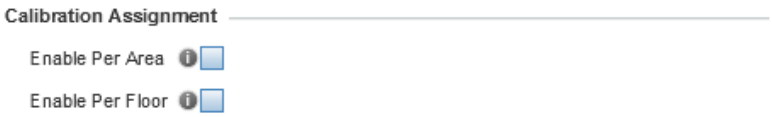
Note: If the Smart RF Policy is disabled but assigned to an RF Domain, the Access Point radio channels will be randomly assigned from the defined Channel Settings in the Channel and Power configuration screen. The transmit power for each radio will be set to the maximum permitted value.

2.1.2 Group By

The Group By parameters determines if the APs are further grouped by Area or Floor when making Smart RF calculations. Each AP is assigned to an RF Domain which determines how the APs are organized and managed within a WiNG 5 system. The APs can be further placed into Areas and Floors under an RF Domain (if desired) to further simplify the management and visualization of the APs at a site.

By default the grouping is disabled which results in Smart RF calculations being performed across all the Smart RF managed radios in an RF Domain regardless if the APs are deployed in different buildings or floors. When grouping by Area or Floor is enabled, the Smart RF managed radios will only form neighbor relationships with other Smart RF managed radios in their assigned Area or Floor. This results in Smart RF calculations and decisions being coordinated between the APs within each defined Area or Floor.

Web-UI



CLI Command Syntax

```
[no] group-by area
[no] group-by floor
```

The grouping of APs can be especially useful for multi-floor deployments when it's desirable to have Smart RF calculations to operate independently on each floor. For example assume a customer has a large high-rise office building where Wi-Fi users reside across 4 floors. All the APs in the building are assigned to a single RF Domain, however by default Smart RF will operate assuming all the APs are deployed on the same coverage area. By assigning the APs to different floors under the RF Domain and enabling the Per Floor grouping, the Smart RF calculations will now be coordinated between the Smart RF managed radios on each floor.

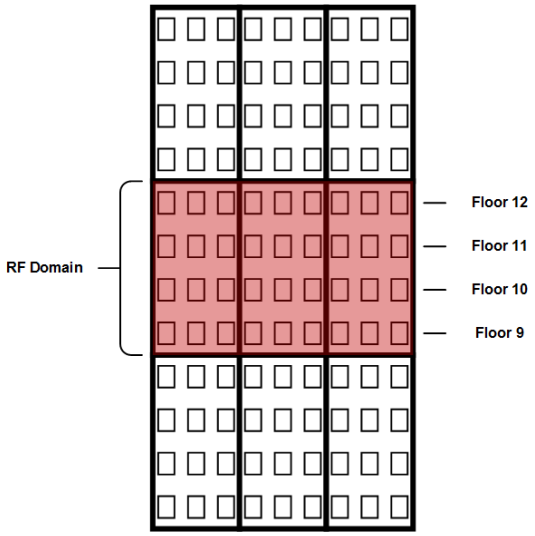


Figure 2.1.2 – Per Floor Grouping Example

2.2 Channel and Power

The Channel and Power screen in the Smart RF Policy includes the following configuration sections:

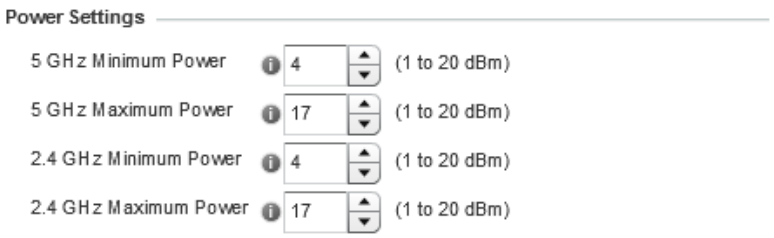
- ***Power Settings*** – Determines the minimum and maximum transmit power values assigned to Smart RF managed radios.
- ***Channel Settings*** – Determines the pool of channels and channel widths assigned to the Smart RF managed radios.

2.2.1 Power Settings

The Power Settings parameters determines the minimum and maximum power values (in dBm) that can be assigned to 2.4 GHz and 5 GHz Smart RF managed radios. By default each 2.4 GHz and 5 GHz will be assigned a transmit power value between 4 – 17 dBm which can be configured by modifying the Minimum Power and Maximum Power parameters for each radio type.

As a general best practice recommendation it is not recommended that you increase the Maximum Power values for the 2.4 GHz or 5 GHz radios beyond the default 17 dBm value. The default value has been defined to provide a 3 dBm margin for the Neighbor Recovery and Coverage Hole Recovery features. If each radio in the system is operating at a maximum of 20 dBm, the Smart RF managed radios will be unable to increase their transmit power if a neighboring AP fails or a coverage hole is detected. You should only increase the Maximum Power values if the Neighbor Recovery and Coverage Hole Recovery features are disabled.

Web-UI



CLI Command Syntax

```
assignable-power <2.4GHz|5GHz> min <1-20>
assignable-power <2.4GHz|5GHz> max <1-20>
```

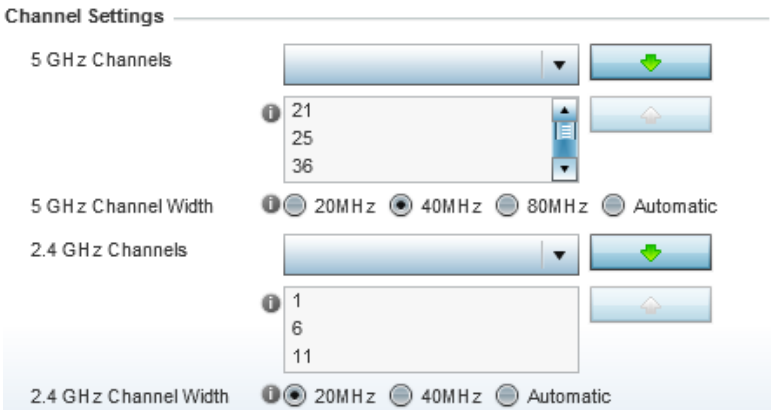
2.2.2 Channel Settings

The Channel Settings parameters define the pool of channels that can be assigned to the 2.4 GHz and 5 GHz Smart RF managed radios in addition to the channel width (20 MHz, 40 MHz or 80 MHz). By default the 2.4 GHz radios will be assigned a 20 MHz wide channel while the 5 GHz radios will be assigned a 40 MHz wide channel. The 80 MHz wide channel is only supported by the newer 802.11ac radios.

- ***2.4 GHz Radios*** – Smart RF will assign a 20 MHz wide channel (1, 6 or 11) to each Smart RF managed radio
- ***5 GHz Radios*** – Smart RF will assign a permitted 40 MHz channel (21, 25, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165 or 173) to each Smart RF managed radio

As a best general practice it is recommended that you use the default Channel Widths as the default parameters will support legacy 802.11a/b/g devices in addition to newer 802.11n/ac devices. While Smart RF will assign a 40 MHz wide channel to the 5 GHz radios, this will not prevent 20 MHz capable device from associating as both 20 MHz and 40 MHz devices can coexist.

Web-UI



CLI Command Syntax

```
channel-list <2.4GHz|5GHz> <comma-separated-list-of-channels>
channel-width <2.4GHz|5GHz> (20MHz|40MHz|80MHz|auto)
```

For the 5 GHz Smart RF managed radios it may be desirable to remove certain channels from the available channel list. For example it may be desirable to remove channels subject to Dynamic Frequency Selection (DFS) to minimize the impact to Wi-Fi clients if a radar is detected. It may also be desirable to remove certain channels for Voice handsets to optimize roaming or legacy 802.11a devices which do not support the U-NNI high band.

Note: Later versions of WiNG support Area Based Channel Settings allowing lists of channels to be assigned to Access Points in a specific area. For example this would allow an administrator to assigning different channels to indoor vs. outdoor Access Points.

*TIP: You can view the supported channels / power values per device by issuing the **show wireless regulatory device-type <AP Model> <ISO-3166 Country Code>** command.*

2.3 Scanning Configuration

The Scanning Configuration screen in the Smart RF Policy includes the following configuration sections:

- ***Monitoring Configuration*** – Enables / disables Off-Channel Scanning (OCS) for Neighbor Recovery and Interference Recovery features.
- ***OCS Monitoring Awareness*** – Overrides Off-Channel Scanning (OCS) client awareness during scheduled times.
- ***Scanning Configuration*** – Determines the frequency of Off-Channel Scanning (OCS), which channels are scanned in addition to how Smart RF uses OCS when Voice or Power Save Poling Wi-Fi clients are detected.

2.3.1 Monitoring Configuration

The Smart Monitoring Enable parameter determines if Off-Channel Scanning (OCS) is enabled or disabled on the Smart RF managed radios. Enabled by default, this parameter allows Smart RF managed radios to monitor their coverage areas for the Neighbor Recovery and Interference Recovery features.

Web-UI

CLI Command Syntax

```
[no] smart-ocs-monitoring
```

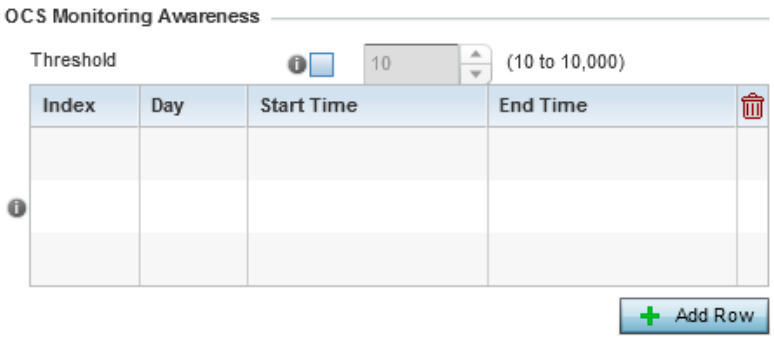
2.3.2 OCS Monitoring Awareness

Smart RF relies on Off-Channel Scanning (OCS) to monitor the RF environment in real-time allowing the Smart RF managed radios to adapt to changes in the RF environment in real-time. Smart RF managed radios that go off-channel can impact certain devices, therefore Smart RF is adaptive in that by default it will prevent OCS on a Smart RF managed radio if it detects an active voice call or if packets are queued for Power Save Polling (PSP) clients.

Voice and PSP awareness is set to dynamic by default. When in dynamic mode only when a voice call is in progress or packets are queued for PSP clients does a Smart RF managed radio avoid going off-channel. You can also set Voice or PSP awareness to strict mode if required which will prevent OCS if a Voice or PSP Wi-Fi client is associated to a Smart RF managed radio. Additionally you can define a Client Aware Scanning threshold for 2.4 GHz and 5 GHz radios to determine the number of associated Wi-Fi clients on a given Smart RF managed radio to prevent OCS.

If the deployment includes Wi-Fi devices that support PSP or Voice, some Smart RF managed radios may not be able to go off-channel for an extended period of time which means those radios may not have the current interference or neighbor data. The OCS Monitoring Awareness feature allows administrators to schedule up to three timeslots for when PSP and Voice awareness parameters can be ignored thus allowing the Smart RF radios to go off-channel and gather the current RF data.

Web-UI



CLI Command Syntax

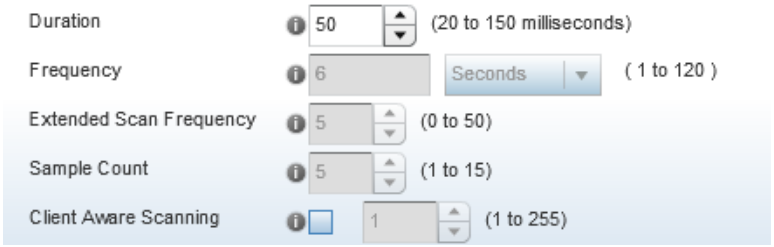
```
smart-ocs-monitoring awareness-override schedule <1-3> <START> <END> <DAY>
       <START> - Start Time using HH:MM format
       <END> - End Time using HH:MM format
       <DAY> - Day when the schedule is active (all|mon|tue|wed|thu|fri|sat|sun)
```

2.3.3 Scanning Configuration (2.4 GHz / 5 GHz)

The Scanning Configuration determines the Off-Channel Scanning (OCS) configuration parameters assigned to the 2.4 GHz and 5 GHz Smart RF managed radios. The values for the Frequency, Extended Scan and Sample Count are automatically assigned to the most optimum values based on the Sensitivity value selected in the Basic Configuration screen. These values can also be modified when setting the Sensitivity value to Custom.

The Client Aware Scanning parameter can also be optionally enabled to determine a threshold for the number of associated Wi-Fi clients on a Smart RF managed radio before it avoids going off-channel.

Web-UI



CLI Command Syntax

```
smart-ocs-monitoring off-channel-duration <2.4GHz|5GHz> <20-150>
smart-ocs-monitoring frequency <2.4GHz|5GHz> <1-120>
smart-ocs-monitoring extended-scan-frequency <2.4GHz|5GHz> <0-50>
smart-ocs-monitoring sample-count <2.4GHz|5GHz> <1-15>
smart-ocs-monitoring client-aware <2.4GHz|5GHz> <1-255>
```

The Duration, Frequency, Extended Scan Frequency and Sample count values determine how often and long Smart RF managed radios go off-channel and how much data is recorded. The following table provides a detailed overview of each OCS parameter:

Parameter	Description
Duration	The amount of time in milliseconds Smart RF managed radios remain off-channel when they perform a scan. The default setting is 50 milliseconds for both the 2.4 GHz and 5 GHz radios.
Frequency	The frequency in which Smart RF managed radios change channels for an off-channel scan. The default setting is 6 seconds when a Medium Sensitivity is selected.
Extended Scan Frequency	Smart RF will perform an off-channel scan of a single channel every 6 seconds with a total of 10 off-channel scans in a one-minute period. Every nth time (extended-scan-frequency value) the Smart RF managed radio will perform an extended scan of the environment as a whole, including outside noise factors. The default is 5 when a Medium Sensitivity is selected.
Sample Count	The number of samples each Smart RF managed radio takes before reporting to the elected RF Domain Manager (RFDM). The default is 5 samples for the 5 GHz radios and 10 samples for the 2.4 GHz radios when a Medium Sensitivity is selected.

Table 2.3.3 – Scanning Configuration

TIP: You can calculate how long it will take each Smart RF managed radio to report to the elected RF Domain Manager by using the following formula: FREQUENCY x SAMPLE-COUNT x NUM-CHANNELS.

For example a 2.4 GHz radio will take 180 seconds (6x10x3 = 180).

2.3.3.1 Power Save Aware Scanning

The Power Save Aware Scanning parameter allows Smart RF managed radios to detect Wi-Fi clients in power-save mode and take them into consideration when performing off-channel scans. By default each Smart RF managed radio is set to Dynamic and each radio will consider wireless clients in a Power Save Polling (PSP) state and may postpone the off-channel scan until the Wi-Fi client awakens at the DTIM interval. If set to Strict the Smart RF managed radios will not perform an off-channel scan when a PSP Wi-Fi client is detected.

Web-UI

CLI Command Syntax

```
smart-ocs-monitoring power-save-aware <2.4GHz|5GHz> (dynamic|strict|disable)
```

This parameter may be set to Strict in an environment where off-channel scanning may interfere with the DTIM and clients waking to receive data. For example, warehouse environments related to logistics / shipping where there may be hundreds of handheld devices scanning thousands of packages in a given shift. These clients alternate between power-save mode and awake constantly and thus, it would be beneficial to set the Power Save Aware Scanning mode set to Strict.

2.3.3.2 Voice Aware Scanning

As with Power Save Aware Scanning, Voice Aware Scanning allows Smart RF managed radios to delay off-channel scanning when Voice clients are present on the network. In a mixed client environment, the default setting of Dynamic is sufficient, however if a Wireless LAN is dedicated to Voice it is recommended that the setting be set to Strict.

Web-UI

CLI Command Syntax

```
smart-ocs-monitoring voice-aware <2.4GHz|5GHz> (dynamic|strict|disable)
```

2.4 Recovery

The Recovery screen in the Smart RF Policy includes the following configuration sections:

- ***Neighbor Recovery*** – Determines the hold-time, thresholds and sampling values for the Neighbor Recovery feature.
- ***Interference Recovery*** – Determines the noise factor, thresholds and hold-times and deltas for the Interference Recovery feature.
- ***Coverage Hole Recovery*** – Determines the thresholds and intervals for the Coverage Hole Recovery feature.

2.4.1 Neighbor Recovery

2.4.1.1 Hold Time

The Power Hold Time parameter determines the time in seconds a Smart RF managed radio waits between two power changes. By default the Power Hold Time parameter value is set to 0 (disabled) when the Sensitivity is set to Medium in the Basic Configuration screen. The value can be modified when the Sensitivity is set to Custom.

Web-UI

CLI Command Syntax

```
neighbor-recovery power-hold-time <0-3600>
```

2.4.1.2 Neighbor Recovery

The Neighbor Power Threshold parameters determine the maximum power increase threshold used by each Smart RF managed radio if the radio is required to increase its power to compensate for a failed neighbor. By default the Neighbor Thresholds for both 2.4 GHz and 5 GHz radios is set to -70 dBm when the Sensitivity is set to Medium in the Basic Configuration screen. These value can be modified when the Sensitivity is set to Custom.

Web-UI

CLI Command Syntax

```
neighbor-recovery power-threshold <2.4GHz|5GHz> <-85--55>
```

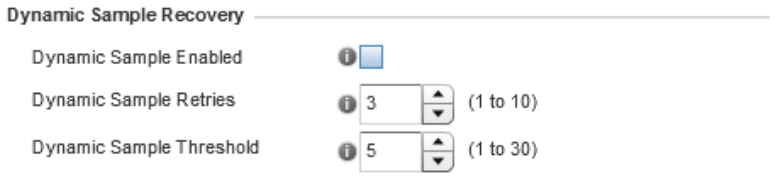
Optimal radio power settings are derived by determining the attenuation of all Smart RF neighbors for a given radio. A Smart RF probe is transmitted by each Smart RF managed radio and then the RSSI of each neighbor response is sent to the elected RF Domain Manager (RFDM). Based on Off-Channel Scanning (OCS) Sample Count in the Scanning and Configuration screen, an average RSSI for each neighbor is determined and from that the overall attenuation of the neighbors. The attenuation + power threshold is our power setting. So if a neighbor attenuation is calculated at 80 and the threshold is set to -70, the radio power will be set to 10 (80+(-70) = 10).

In environments that have excessive obstructions where neighboring radios may not be heard as well, the Power Threshold may be lowered (example -65) in order to arrive at a better overall power setting.

2.4.1.3 Dynamic Sample Recovery

The Dynamic Sampling Recovery parameters enables an administrator to define how Smart RF adjustments are triggered by locking retry and threshold values. This parameter is disabled by default but can be enabled by selecting the Dynamic Sample Enabled checkbox.

Web-UI



CLI Command Syntax

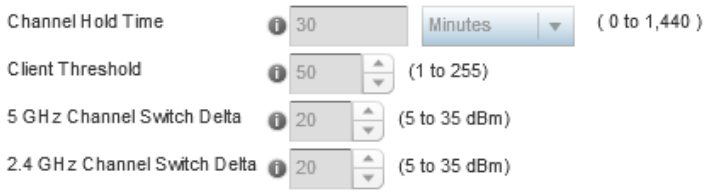
```
[no] neighbor-recovery dynamic-sampling
neighbor-recovery dynamic-sampling retries <1-10>
neighbor-recovery dynamic-sampling threshold <1-30>
```

When Dynamic Sampling is enabled, the Smart RF managed radios perform extra sampling to avoid excessive power changes. The Smart RF managed radios keep track of the number of samples that were processed without a power change. If a power change has not occurred in a while and the Dynamic Sample Threshold has been exceeded, the Smart RF Managed radio can perform a power change immediately. If a power change has occurred recently and another power changed is required (within Dynamic Sample Threshold), the Smart RF managed radio sends additional samples (Dynamic Sample Retry) to see if the power change is still required and the power is changed only after confirming it is required.

2.4.2 Interference Recovery

The Interference Recovery feature performs channel changes when noise from neighboring Wi-Fi devices or outside interference is detected and the delta between the current channel energy and the perceived energy from other signals falls below a threshold. The Channel Hold Time, Client Threshold and Channel Switch Delta parameters are automatically assigned the optimum values based on the Sensitivity value selected in the Basic Configuration screen. These values can also be modified when setting the Sensitivity value to Custom.

Web-UI



CLI Command Syntax

```
interference-recovery channel-hold-time <0-86400>
interference-recovery client-threshold <1-255>
interference-recovery channel-switch-delta <2.4GHz|5GHz> <5-35>
```

The following table provides a detailed overview of each important Interference Recovery parameters which can be defined for both 2.4 GHz and 5 GHz Smart RF managed radios:

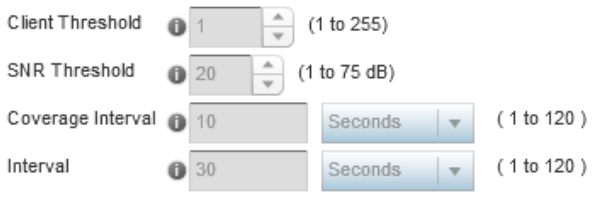
Parameter	Description
Channel Hold Time	The minimum amount between two channel changes due to interference on a Smart RF managed radio. The default is 30 minutes when a Medium Sensitivity is selected.
Client Threshold	The number of Wi-Fi clients for which a Smart RF managed radio will not perform a channel change due to interference. The default is 50 clients when a Medium Sensitivity is selected.
2.4 GHz Channel Switch Delta	The minimum expected between the perceived energy on the 2.4 GHz radios current channel compared to that of the best possible alternate channel. The default is 20 dBm when a Medium Sensitivity is selected.
5 GHz Channel Switch Delta	The minimum expected between the perceived energy on the 5 GHz radios current channel compared to that of the best possible alternate channel. The default is 20 dBm when a Medium Sensitivity is selected.

Table 2.4.2 – Interference Recovery

2.4.3 Coverage Hole Recovery

The Coverage Hole feature performs power changes when Wi-Fi devices connectivity falls below a defined SNR threshold. The Client Threshold, SNR threshold, Coverage Interval and Interval parameters are automatically assigned the optimum values based on the Sensitivity value selected in the Basic Configuration screen. These values can also be modified when setting the Sensitivity value to Custom.

Web-UI



CLI Command Syntax

```
coverage-hole-recovery client-threshold <2.4GHz|5GHz> <1-255>
coverage-hole-recovery snr-threshold <2.4GHz|5GHz> <1-75>
coverage-hole-recovery coverage-interval <2.4GHz|5GHz> <1-20>
coverage-hole-recovery interval <2.4GHz|5GHz> <1-120>
```

The following table provides a detailed overview of each important Coverage Hole Recovery parameters which can be defined for both 2.4 GHz and 5 GHz Smart RF managed radios:

Parameter	Description
Client Threshold	Defines the number of Wi-Fi clients detected that fall below the SNR threshold before recovery takes place. The default is 1 client when a Medium Sensitivity is selected. This setting can be modified as it may not be desirable to adjust power every time a single Wi-Fi client falls before the defined SNR threshold.
SNR Threshold	Defines the minimum signal-to-noise ratio heard from the Wi-Fi client before recovery takes place. The default is 20 dB when a Medium Sensitivity is selected. As a best practice is it never recommended to set the SNR below 20 dB. When Wi-Fi clients are detected below the defined SNR, recovery will take place.
Coverage Interval	Defines the interval coverage hole recovery should be initiated by a Smart RF managed radio when a coverage hole is detected. The default is 10 seconds when a Medium Sensitivity is selected. When a coverage hole has been detected and recovery is taking place, the detection becomes more aggressive in determining if the coverage hole still exists.
Interval	Defines the interval in which coverage hole detection takes place by a Smart RF managed radio. The default is 30 seconds when a Medium Sensitivity is selected. Note that this interval may need to be lowered in environments such as warehouses where coverage is critical (i.e. low cell count, large cell size).

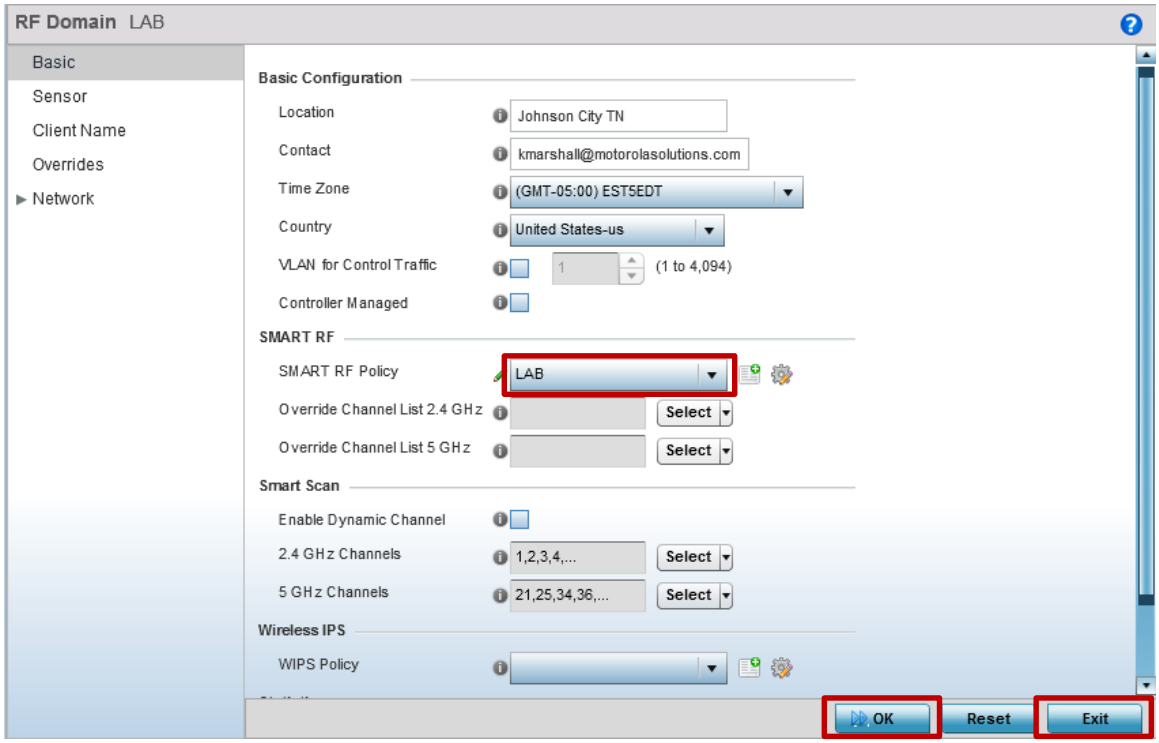
Table 2.4.3 – Coverage Hole Recovery

2.5 RF Domain

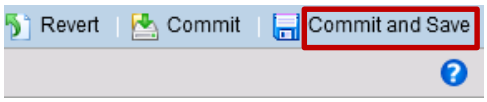
Smart RF Policies are assigned to radios using RF Domains and each RF Domain supports one Smart RF Policy. Smart RF Policies can be assigned to an RF Domain using either the CLI or Web-UI. The following procedure describes how to create a new Smart RF Policy using the Web-UI:

1 **Select *RF Domains → <rf-domain-name>* then click *Edit*. In the *Basic* screen assign the desired *SMART RF Policy* then click *OK* and *Exit*:**

Configuration → RF Domains → <rf-domain> → Basic



2 **Select *Commit and Save*:**



The following procedure describes how to assign a Smart RF Policy to a RF Domain using the CLI:

Enable Privileged Context:

```
RFS4000-1> enable
```

Enter the Configuration Context:

```
RFS4000-1# configure terminal
```

Access the RF Domain Configuration Context:

```
RFS4000-1(config)# rf-domain <name>
```

Assign a Smart RF Policy to the RF Domain:

```
RFS4000-1(config-rf-domain-<name>)# use smart-rf-policy <name>
```

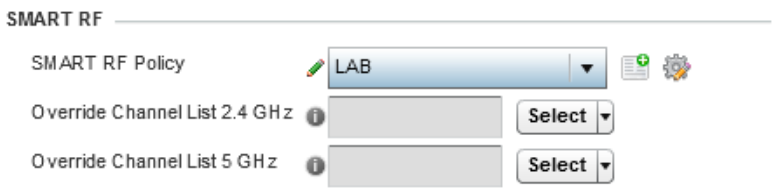
Commit and Save the changes:

```
RFS4000-1(config-rf-domain-<name>)# commit write
```

2.5.1 RF Domain Overrides

For each RF Domain WiNG 5 supports the ability to override the pool of 2.4 GHz and 5 GHz channels which can be assigned to Smart RF Managed radios. This allows administrators to assign a global Smart RF Policy across all the RF Domains (sites) in the system but define specific pools of channels which can be assigned to Smart RF managed radios for each site. For example an administrator may assign different pools of 5 GHz channels to sites in North America vs. Europe using an RF Domain override vs. defining separate Smart RF Policies for each region.

Web-UI



CLI Command Syntax

```
Override-smartrf channel-list <2.4GHz|5GHz> <comma-separated-list-of-channels>
```

2.6 System Events

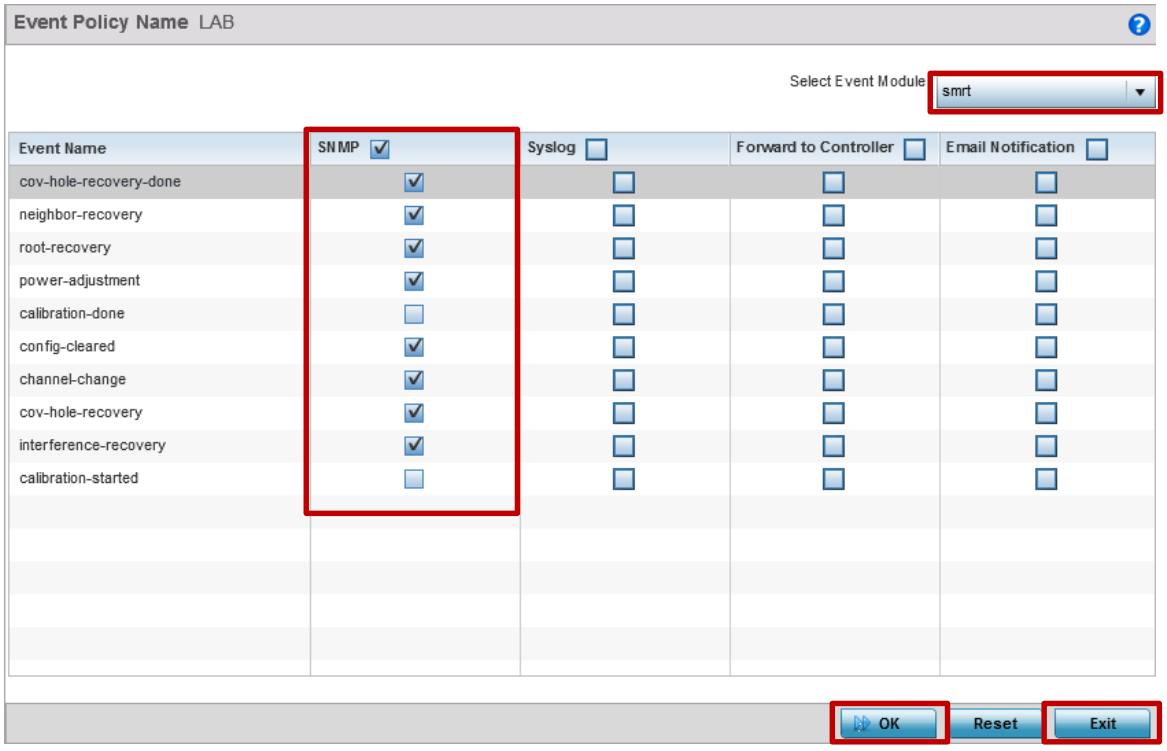
By default all Smart RF events are aggregated for forwarded to the Controller, and if logging is enabled each Smart RF event will be captured in the System Event log. If a SNMP trap receiver is defined in the Management Policy assigned to the Controller, each Smart RF Event by default will also be forwarded as a SNMP trap to the defined SNMP trap receiver.

You can determine how Smart RF events are logged and forwarded in WiNG 5 by defining an Event Policy using the CLI or Web-UI and assigning it to the Controller Profile. Each Event Policy includes a list of WiNG 5 events that are groped in modules. For each event you can determine if the event is ignored or forwarded as an SNMP trap, syslog message or an Email Notification when the event occurs.

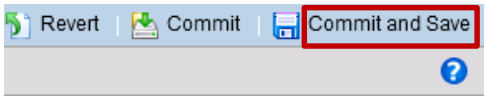
The following procedure describes how to enable Smart RF events in an Event Policy named LAB using Web-UI. In this example specific Smart RF events will be configured to be forwarded as SNMP traps when the Smart RF event occurs:

1 **Select *Devices* → *Event Policy* → *<policy-name>* then select the *Event Module* named *smrt*. For each event select if the event is forwarded as an *SNMP* trap, *Syslog* message or *Email Notification*. Click *OK* then *Exit*:**

Configuration* → *Devices* → *Event Policy* → *<policy-name>* → *smrt



2 **Select *Commit and Save*:**



The following procedure describes how to enable Smart RF events in an Event Policy named LAB using CLI. In this example specific Smart RF events will be configured to be forwarded as SNMP traps when the Smart RF event occurs:

Enable Privileged Context:

```
RFS4000-1> enable
```

Enter the Configuration Context:

```
RFS4000-1# configure terminal
```

Access the System Event Policy Configuration Context:

```
RFS4000-1(config)# event-system-policy LAB
```

Enable one or more Smart RF Events as SNMP traps:

```
RFS4000-1(config-<path>)# event smrt cov-hole-recovery-done snmp on
RFS4000-1(config-<path>)# event smrt neighbor-recovery snmp on
RFS4000-1(config-<path>)# event smrt root-recovery snmp on
RFS4000-1(config-<path>)# event smrt power-adjustment snmp on
RFS4000-1(config-<path>)# event smrt calibration-done snmp off
RFS4000-1(config-<path>)# event smrt config-cleared snmp on
RFS4000-1(config-<path>)# event smrt channel-change snmp on
RFS4000-1(config-<path>)# event smrt cov-hole-recovery snmp on
RFS4000-1(config-<path>)# event smrt interference-recovery snmp on
RFS4000-1(config-<path>)# event smrt calibration-started snmp off
```

Commit and Save the changes:

```
RFS4000-1(config-<path>)# commit write
```

Note: In the above example the System Event Policy named LAB has been assigned to the RFS 4000s Profile named LAB-RFS4000. Additionally a SNMPv3 Trap Receiver has been defined in the Management Policy named CONTROLLERS also assigned to the RFS 4000 Profile.

2.7 Clearing Smart RF Configuration

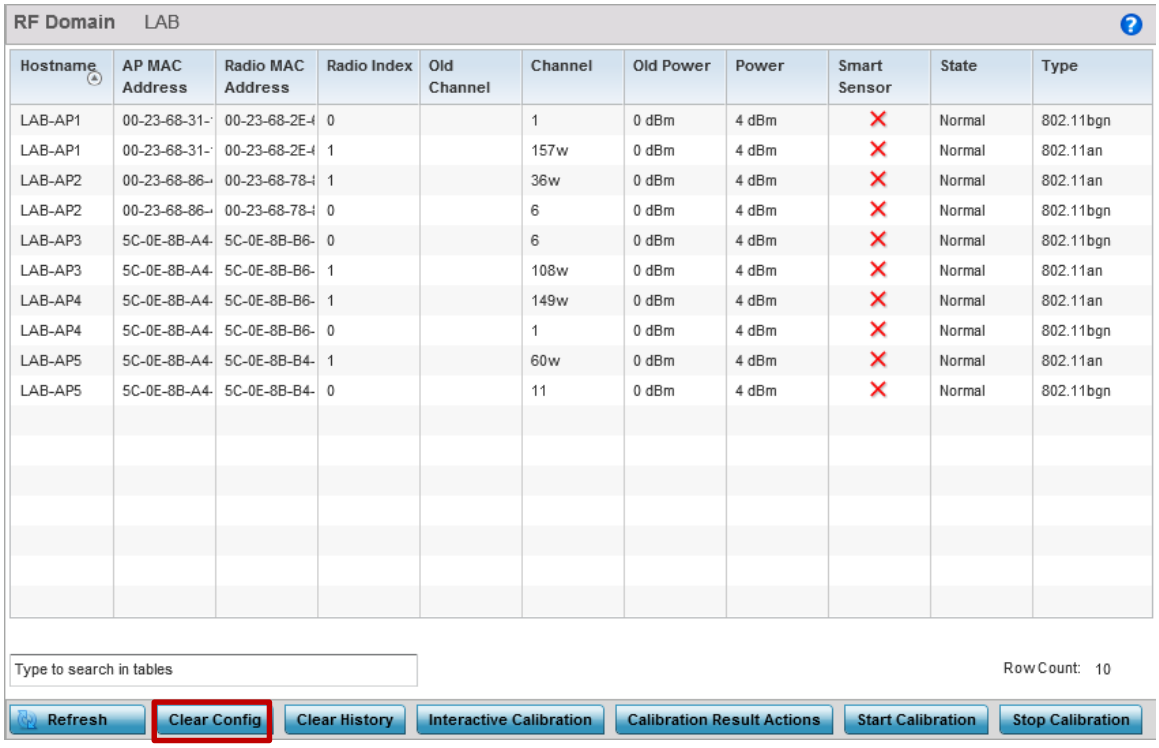
While Smart RF managed radios are optimized in real-time as the RF environment changes, over time it may be desirable to reset the Smart RF configuration for a site so that all the Smart RF managed radios re-converge with new channel and power values.

This is achieved by clearing the Smart RF configuration per site (RF Domain) using the CLI or Web-UI. When the Smart RF configuration is cleared for a site, it can take anywhere from 15 – 20 minutes for each of the Smart RF managed radios to re-converge with new optimum channel and power values. As the re-convergence can be impacting to Wi-Fi devices, it is only recommended that the clear of the Smart RF configuration during a scheduled maintenance window.

The following procedure describes how to clear the Smart RF configuration for a site (RF Domain) using the Web-UI:

1 **Select *Operations → <rf-domain-name> → SMART RF*. At the bottom of the screen select *Clear Config*. This will clear the current Smart RF configuration and cause the Smart RF radios to re-converge with new channel and power configurations:**

Operations → <rf-domain-name> → SMART RF



*Note: You should NEVER select the **Interactive Calibration** or **Start Calibration** options. These are depreciated features inherited from the older WiNG 4.X release and should NOT be used in a WiNG 5 deployment.*

The following procedure describes how to clear the Smart RF configuration for a site (RF Domain) using the CLI:

Enable Privileged Context:

```
RFS4000-1> enable
```

Clear the Smart RF Configuration for a Site:

```
RFS4000-1# service smart-rf clear-config on <rf-domain-name>
```

*Note: You should NEVER issue the **service smart-rf interactive-calibration** or **service smart-rf run-calibration** commands. These are depreciated features inherited from the older WiNG 4.X release and should NOT be used in WiNG 5.*

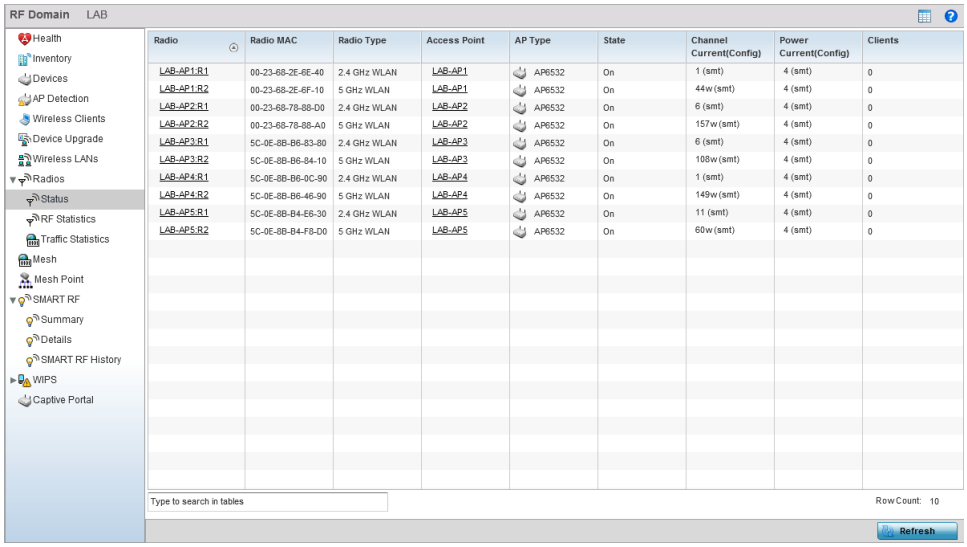
3. Verification & Troubleshooting

The following section highlights useful statistics and CLI commands that can be used to verify the operation and aid in troubleshooting a Smart RF environment.

3.1 Channel & Power Assignments

Channel and power values for Smart RF managed radios can be viewed per RF Domain in real-time in both the CLI and Web-UI. By default each radio is configured to be Smart RF managed and will display (smt) next to its channel and power configuration. If the radio does not display (smt), this indicates that a static channel and/or power value has been assigned to the radio.

Statistics → <rf-domain> → Radios → Status



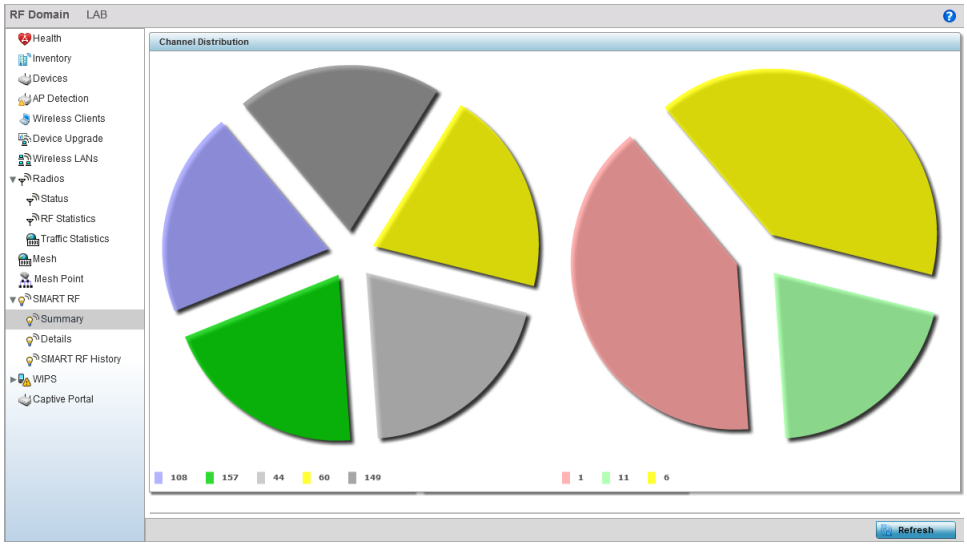
Command Line Interface

```
RFS4000-1# show wireless radio on <rf-domain-name>

================================================================================================
RADIO                RADIO-MAC             RF-MODE        STATE       CHANNEL     POWER #CLIENT
------------------------------------------------------------------------------------------------
LAB-AP1:R1           00-23-68-2E-6E-40 2.4GHz-wlan          On      1 (  smt)  4 (smt)        0
LAB-AP1:R2           00-23-68-2E-6F-10   5GHz-wlan          On    44w (  smt)  4 (smt)        0
LAB-AP2:R1           00-23-68-78-88-D0 2.4GHz-wlan          On      6 (  smt)  4 (smt)        0
LAB-AP2:R2           00-23-68-78-88-A0   5GHz-wlan          On  157w (  smt)  4 (smt)        0
LAB-AP3:R1           5C-0E-8B-B6-83-80 2.4GHz-wlan          On      6 (  smt)  4 (smt)        0
LAB-AP3:R2           5C-0E-8B-B6-84-10   5GHz-wlan          On  108w (  smt)  4 (smt)        0
LAB-AP4:R1           5C-0E-8B-B6-0C-90 2.4GHz-wlan          On      1 (  smt)  4 (smt)        0
LAB-AP4:R2           5C-0E-8B-B6-46-90   5GHz-wlan          On  149w (  smt)  4 (smt)        0
LAB-AP5:R1           5C-0E-8B-B4-E6-30 2.4GHz-wlan          On     11 (  smt)  4 (smt)        0
LAB-AP5:R2           5C-0E-8B-B4-F8-D0   5GHz-wlan          On    60w (  smt)  4 (smt)        0
================================================================================================
Total number of radios displayed: 10
```

3.2 Channel Distribution

2.4 GHz and 5 GHz channel distribution for Smart RF managed radios can be viewed in real-time per RF Domain using the CLI and Web-UI. The channel distribution statistics are useful for ensuring that the 2.4 GHz and 5 GHz channels are evenly distributed throughout the site, however depending on the number of Access Points (APs) and the RF environment (interference / noise), equal distribution is not always possible.

Statistics → <rf-domain> → SMART RF → Summary → Channel Distribution



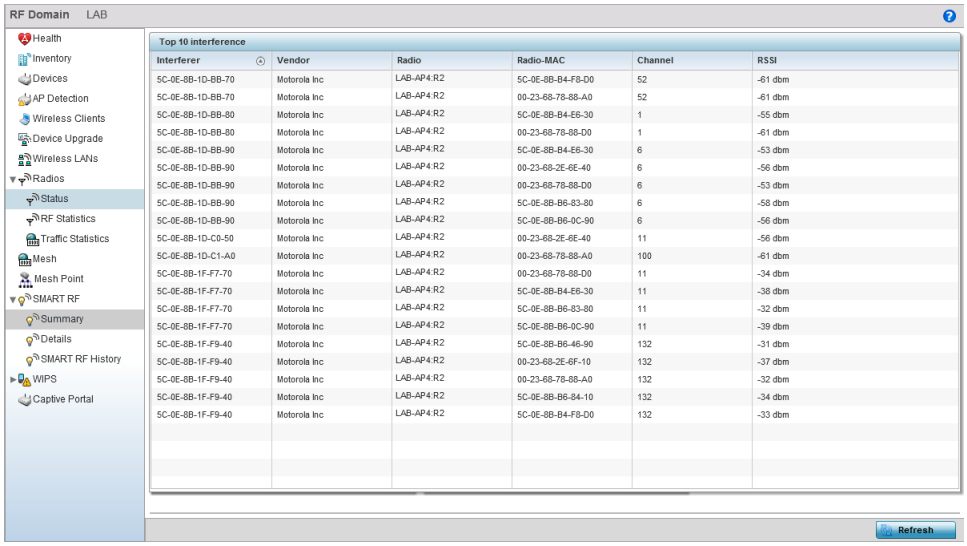
Command Line Interface

```
RFS4000-1# show smart-rf channel-distribution on <rf-domain-name>

2.4GHz channel distribution for 5 radios
-------------------------------------
 CHANNEL  NUM RADIOS  DISTRIBUTION (%)
-------------------------------------
  1        2           40.00
  6        2           40.00
  11       1           20.00
-------------------------------------

5GHz channel distribution for 5 radios
-------------------------------------
 CHANNEL  NUM RADIOS  DISTRIBUTION (%)
-------------------------------------
  44w      1           20.00
  60w      1           20.00
  108w     1           20.00
  149w     1           20.00
  157w     1           20.00
-------------------------------------
```

3.3 Interferering Access Points

A list of Interfering Access Points can be view per RF Domain in real-time using the CLI and Web-UI. Each Smart RF managed radio will capture the MAC address, Vendor (if available), Channel and RSSI of each Interfering Wi-Fi Access Point that it sees. This can be useful when tracking down older Access Points at a site which should have been de-commission but are still powered and beaconing which can cause mobility and RF performance issues at a site.

Statistics → <rf-domain> → SMART RF → Top 10 Interference



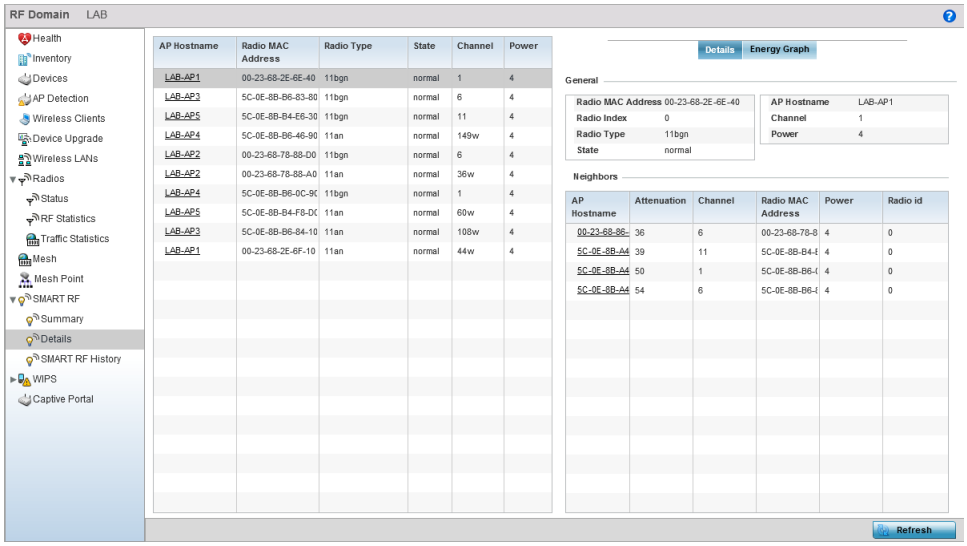
Command Line Interface

```
RFS4000-1# show smart-rf interfering-ap on <rf-domain-name>

-------------------------------------------------------------------------------
      INTERFERER          VENDOR         RADIO          RADIO-MAC       CHNL    RSSI
-------------------------------------------------------------------------------
  5C-0E-8B-1F-F7-70   Motorola Inc   LAB-AP3:R1   5C-0E-8B-B6-83-80   11    -32
  5C-0E-8B-1F-F9-40   Motorola Inc   LAB-AP2:R2   00-23-68-78-88-A0   132   -32
  ..
  ..
  ..
  5C-0E-8B-1D-BB-90   Motorola Inc   LAB-AP1:R1   00-23-68-2E-6E-40   6     -56
  5C-0E-8B-1D-C0-50   Motorola Inc   LAB-AP1:R1   00-23-68-2E-6E-40   11    -56
  5C-0E-8B-1D-BB-90   Motorola Inc   LAB-AP4:R1   5C-0E-8B-B6-0C-90   6     -56
  5C-0E-8B-1D-BB-90   Motorola Inc   LAB-AP3:R1   5C-0E-8B-B6-83-80   6     -58
  5C-0E-8B-1D-BB-70   Motorola Inc   LAB-AP2:R2   00-23-68-78-88-A0   52    -60
  5C-0E-8B-1D-BB-70   Motorola Inc   LAB-AP1:R2   00-23-68-2E-6F-10   52    -60
  5C-0E-8B-1D-BB-70   Motorola Inc   LAB-AP5:R2   5C-0E-8B-B4-F8-D0   52    -61
  5C-0E-8B-1D-BB-80   Motorola Inc   LAB-AP2:R1   00-23-68-78-88-D0   1     -61
-------------------------------------------------------------------------------
```

3.4 Radio Neighbor Details

Each Smart RF managed radio maintains a list of neighboring Access Points (APs) which is used for channel and power assignments as well as Neighbor Recovery. A list of neighboring APs can be displayed per Smart RF managed radio using the CLI or Web-UI. Each Smart RF managed radio will display the neighboring APs hostname, how strongly it sees each neighbor (attenuation) in addition to each neighbor's assigned channel and power value.

Statistics → <rf-domain> → SMART RF → Details → <ap-hostname> → Details



Command Line Interface

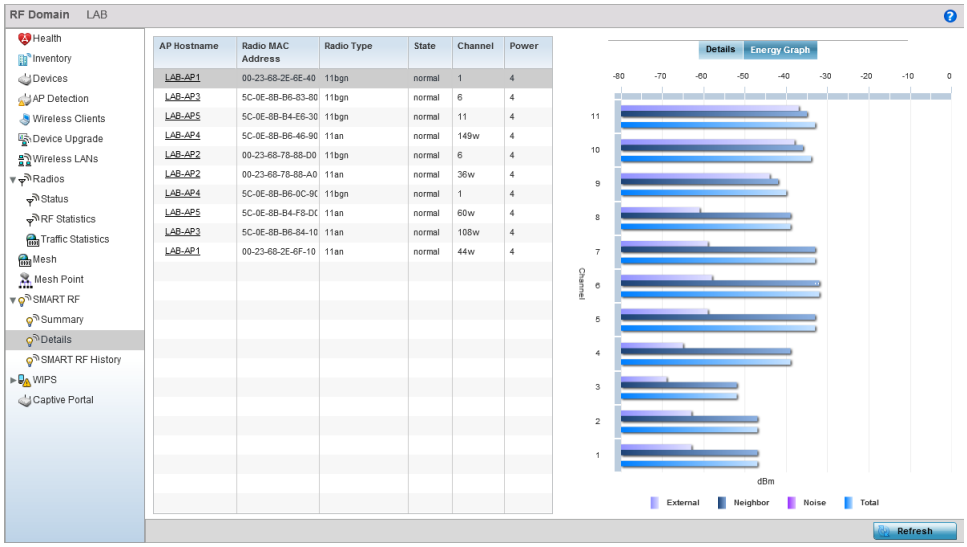
```
RFS4000-1# show smart-rf radio neighbors <radio-mac> on <rf-domain-name>

-------------------------------------------------------------------------------------------
    RADIO          RADIO-MAC       CHNL  NEIGHBORS          MAC          POWER ATTN  CHNL
-------------------------------------------------------------------------------------------
  LAB-AP1:R1   00-23-68-2E-6E-40   1     LAB-AP2:R1   00-23-68-78-88-D0   4      36   6
                                         LAB-AP5:R1   5C-0E-8B-B4-E6-30   4      39   11
                                         LAB-AP4:R1   5C-0E-8B-B6-0C-90   4      50   1
                                         LAB-AP3:R1   5C-0E-8B-B6-83-80   4      54   6


-------------------------------------------------------------------------------------------
```

*TIP: You can also view the neighbors from all 2.4 GHz or 5 GHz radios by issuing the **show smart-rf radio neighbors (all-11an | all-11bgn) on <rf-domain-name>** command.*

3.5 Energy Graphs

Each Smart RF managed radio maintains an energy graph which is used for channel and power assignments as well as Interference Recovery. The energy graph can be displayed per Smart RF managed radio using the CLI or Web-UI. Each radios energy graph will display the External Noise, Neighbors, Noise and Total energy for each channel.

Statistics → <rf-domain> → SMART RF → Details → <ap-hostname> → Energy Graph



Command Line Interface

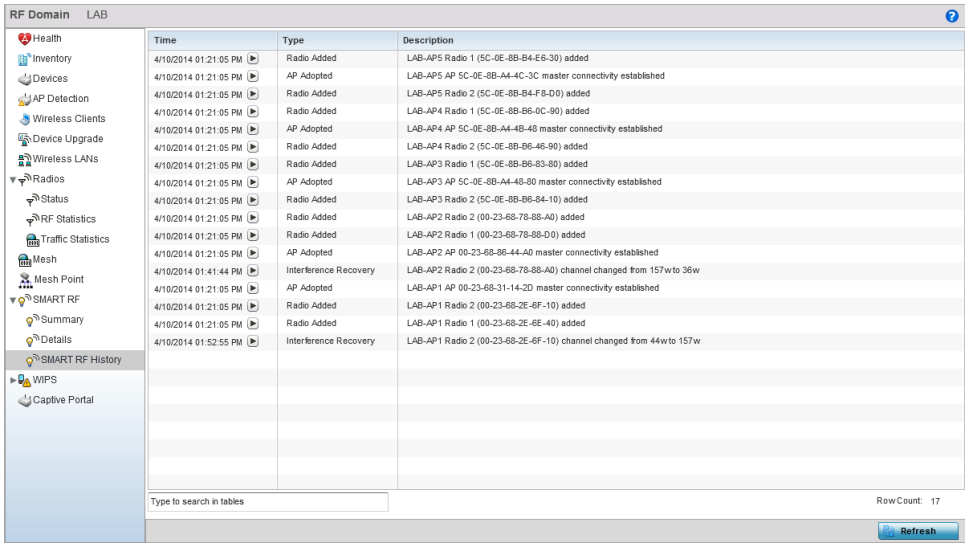
```
RFS4000-1# show smart-rf radio energy <radio-mac> on <rf-domain-name>

Legend - x : External wifi interference  n : Non-Wifi interference
         o : Neighbor wifi interference  # : Total interference
         P : Primary channel             S : Secondary channel

Radio information for : 00-23-68-2E-6E-40 [AP LAB-AP1:Radio 1]
--------------------------------------------------------------------------------
 ch [dbm] S   -80      -70       -60       -50       -40       -30       -20 dbm
--------------+---------+---------+---------+---------+---------+---------+----
              |
              |xxxxxxxxxxxxxxxxx
    1 [ -47] P|ooooooooooooooooooooooooooooooo
              |
              |################################
              |xxxxxxxxxxxxxxxxx
    2 [ -47]  |ooooooooooooooooooooooooooooooo
              |
              |################################
              |xxxxxxxxxxx
    3 [ -52]  |ooooooooooooooooooooooooooo
              |
   ..
   ..
   ..
              |
              |##############################################
              |xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   11 [ -33]  |ooooooooooooooooooooooooooooooooooooooooooooooo
              |
              |##############################################
```

*TIP: You can also view the energy graphs from all 2.4 GHz or 5 GHz radios by issuing the **show smart-rf radio energy (all-11an | all-11bgn) on <rf-domain-name>** command.*

3.6 Smart RF History

The elected RF Domain Manager for each site maintains a history of all Smart RF events which can be displayed in real-time using the CLI or Web-UI. The Smart RF History includes all Smart RF related events including Radios being added, channel and power changes as well as Neighbor Recovery, Interference Recovery and Coverage Hole Recovery events.

Statistics → <rf-domain> → SMART RF → SMART RF History



Command Line Interface

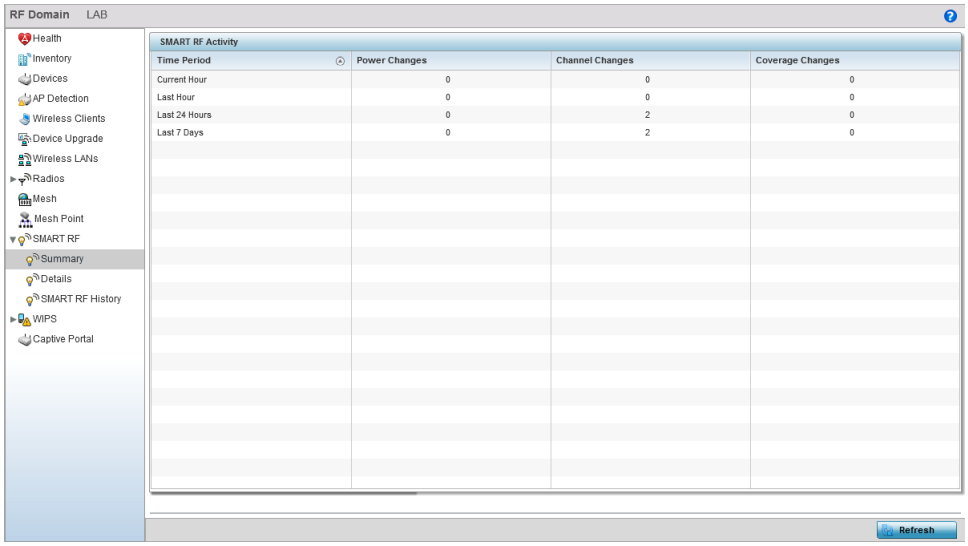
```
RFS4000-1# show smart-rf history on <rf-domain-name>

-------------------------------------------------------------------------------------------------------------
      TIME                      EVENT                      DESCRIPTION
-------------------------------------------------------------------------------------------------------------
2014-04-10 13:52:55    Interference Recovery    Radio LAB-AP1:R2 (00-23-68-2E-6F-10) channel changed from
44w to 157w
                                                Channel change initiated due to excessive neighbor wifi
interference [-47]
2014-04-10 13:41:44    Interference Recovery    Radio LAB-AP2:R2 (00-23-68-78-88-A0) channel changed from
157w to 36w
                                                Channel change initiated due to excessive neighbor wifi
interference [-43]
..
..
2014-04-10 13:21:05    AP Connected             AP LAB-AP4 master connectivity established
-------------------------------------------------------------------------------------------------------------
Total number of history entries displayed: 17
```

*TIP: You can also view the energy graphs from all 2.4 GHz or 5 GHz radios by issuing the **show smart-rf radio energy (all-11an | all-11bgn) on <rf-domain-name>** command.*

3.7 Smart RF History Timeline

The elected RF Domain Manager for each site maintains a history timeline of all Smart RF events which can be displayed in real-time using the CLI or Web-UI. The Smart RF History Timeline provides a summary of Power, Channel and Coverage changes broken down into Current Hour, Last Hour, Last 24 Hours and Last 7 Days. The Smart RF History Timeline is especially useful for identifying sites with excessive changes which can indicate manual intervention is required to permanently mitigate the problem.

Statistics → <rf-domain> → SMART RF → Summary → SMART RF Activity



Command Line Interface

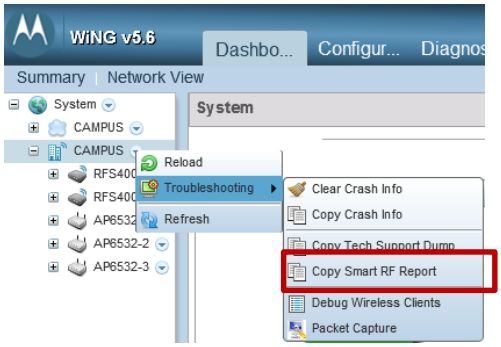
```
RFS4000-1# show smart-rf history-timeline on <rf-domain-name>

Smart-rf timeline of changes for current hour:
-------------------------------------------------
       START TIME       POWER  CHANNEL   COVERAGE
-------------------------------------------------
  2014-04-10 14:00:00    0      0        0
-------------------------------------------------

Smart-rf timeline of changes for last hour:
-------------------------------------------------
       START TIME       POWER  CHANNEL   COVERAGE
-------------------------------------------------
  2014-04-10 13:21:05    0      2        0
-------------------------------------------------

Smart-rf timeline of changes for the past 24 hours of operation:
-------------------------------------------------
       START TIME       POWER  CHANNEL   COVERAGE
-------------------------------------------------
  2014-04-10 14:00:00    0      0        0
  2014-04-10 13:21:05    0      2        0
-------------------------------------------------
  Total Changes          0      2        0

Smart-rf timeline of changes for the past 7 days of operation:
-------------------------------------------------
       START TIME       POWER  CHANNEL   COVERAGE
-------------------------------------------------
  2014-04-10 13:21:05    0      2        0
-------------------------------------------------
  Total Changes          0      2        0
```

3.8 Generate a Smart RF Report

In WiNG 5.4 and above administrators can generate a Smart RF Report using the CLI or Web-UI for each RF Domain which includes the output of various show Smart RF commands. Each Smart RF report includes the current channel / power values, channel distribution, neighbors, activity, history timelines and energy graphs for each Smart RF managed radio. The report is very useful when troubleshooting Smart RF issues for a site as it provides all the necessary Smart RF details in a single ASCII file.

In WiNG 5.4.X and 5.5.X a Smart RF report can only be generated using the CLI, however in WiNG 5.6 and above a Smart RF Report can be generated using both the CLI and Web-UI. When a Smart RF Report is generated it is saved to a TFTP or FTP server as a gzip archive.

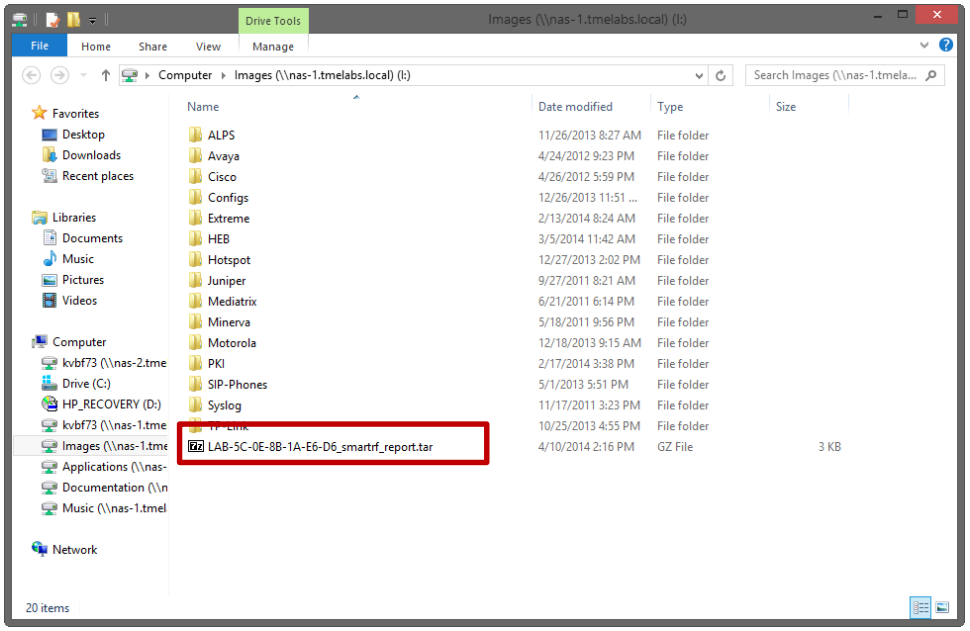
Dashboard → <rf-domain-name> → Troubleshooting → Copy Smart RF Report



Note – WiNG 5.6 and above

Command Line Interface

```
RFS4000-1# remote-debug copy-smart-rf-report rf-domain <rf-domain-name> write
tftp://<tftp-server-ip-address>/<path>/
```



4. Analytics

In WiNG 5.5 introduced Smart RF Analytics support for centrally managed ONEVIEW deployments. Customers with NX 95XX appliances deployed in their data center can enable the Analytics module (free of charge) to capture and display Smart RF statistics at a System, Site or Device level. The Analytics module can capture and display up to 3 months of Smart RF data.

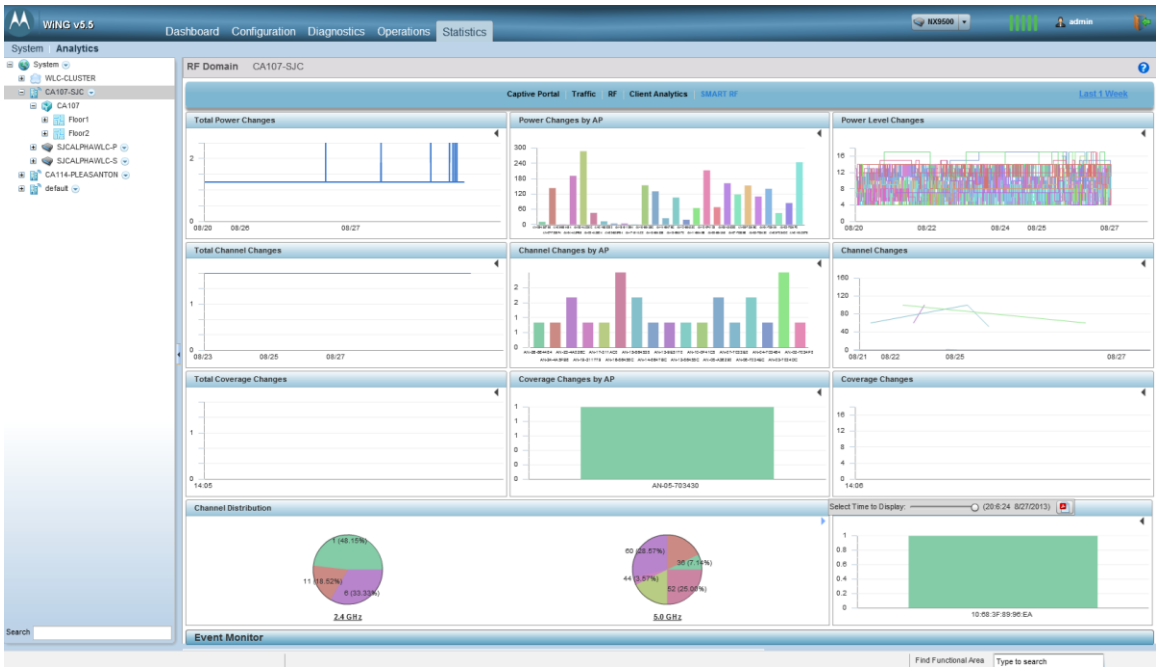


Figure X – Smart RF Analytics

Using this powerful tool administrators can now select the device scope for the Smart RF information they wish to display (System, RF Domain or Device) in addition to a time interval (1 day to 3 months). The information is presented to the administrator in the Web-UI. The Administrator can view the data in graphical format (charts) or in table form. The administrator can also export the data as a PDF report if desired.

The following table highlights the Smart RF data points available from the Analytics Module:

Smart RF Analytics Data Points		
• Total Power Changes	• Total Channel Changes	• Total Coverage Changes
• Power Changes by AP	• Channel Changes by AP	• Coverage Changes by AP
• Power Level Changes	• Channel Changes	• Coverage Changes
• Channel Distribution		

Table X – Analytics Smart RF Data Points

5. Appendix

5.1 Default Smart RF Policy

Default Smart RF Policy (Including Factory Settings)

```
smart-rf-policy LAB
 enable
 no group-by area
 no group-by floor
 sensitivity medium
 assignable-power 5GHz max 17
 assignable-power 5GHz min 4
 assignable-power 2.4GHz max 17
 assignable-power 2.4GHz min 4
 channel-list 5GHz
21,25,36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,15
7,161,165,173
 channel-list 2.4GHz 1,6,11
 channel-width 5GHz 40MHz
 channel-width 2.4GHz 20MHz
 smart-ocs-monitoring
 smart-ocs-monitoring off-channel-duration 5GHz 50
 smart-ocs-monitoring off-channel-duration 2.4GHz 50
 smart-ocs-monitoring frequency 5GHz 6
 smart-ocs-monitoring frequency 2.4GHz 6
 smart-ocs-monitoring sample-count 5GHz 5
 smart-ocs-monitoring sample-count 2.4GHz 10
 smart-ocs-monitoring extended-scan-frequency 5GHz 5
 smart-ocs-monitoring extended-scan-frequency 2.4GHz 5
 smart-ocs-monitoring power-save-aware 5GHz dynamic
 smart-ocs-monitoring power-save-aware 2.4GHz dynamic
 smart-ocs-monitoring voice-aware 5GHz dynamic
 smart-ocs-monitoring voice-aware 2.4GHz dynamic
 no smart-ocs-monitoring client-aware 5GHz
 no smart-ocs-monitoring client-aware 2.4GHz
 no smart-ocs-monitoring awareness-override threshold
 interference-recovery
 interference-recovery noise
 interference-recovery noise-factor 1.5
```

```
interference-recovery neighbor-offset 5
interference-recovery interference
interference-recovery client-threshold 50
interference-recovery channel-switch-delta 5GHz 20
interference-recovery channel-switch-delta 2.4GHz 20
neighbor-recovery
neighbor-recovery power-threshold 5GHz -70
neighbor-recovery power-threshold 2.4GHz -70
coverage-hole-recovery
coverage-hole-recovery interval 5GHz 30
coverage-hole-recovery interval 2.4GHz 30
coverage-hole-recovery coverage-interval 5GHz 10
coverage-hole-recovery coverage-interval 2.4GHz 10
coverage-hole-recovery snr-threshold 5GHz 20
coverage-hole-recovery snr-threshold 2.4GHz 20
coverage-hole-recovery client-threshold 5GHz 1
coverage-hole-recovery client-threshold 2.4GHz 1
interference-recovery channel-hold-time 1800
neighbor-recovery power-hold-time 0
no neighbor-recovery dynamic-sampling
neighbor-recovery dynamic-sampling threshold 5
neighbor-recovery dynamic-sampling retries 3
```

5.2 Running Configuration

Running Configuration

```
!
! Configuration of RFS4000 version 5.5.1.0-017R
!
!
version 2.3
!
!
!
firewall-policy default
 no ip dos smurf
 no ip dos twinge
 no ip dos invalid-protocol
 no ip dos router-advt
 no ip dos router-solicit
 no ip dos option-route
 no ip dos ascend
 no ip dos chargen
 no ip dos fraggle
 no ip dos snork
 no ip dos ftp-bounce
 no ip dos tcp-intercept
 no ip dos broadcast-multicast-icmp
 no ip dos land
 no ip dos tcp-xmas-scan
 no ip dos tcp-null-scan
 no ip dos winnuke
 no ip dos tcp-fin-scan
 no ip dos udp-short-hdr
 no ip dos tcp-post-syn
 no ip dos tcphdrfrag
 no ip dos ip-ttl-zero
 no ip dos ipspoof
 no ip dos tcp-bad-sequence
 no ip dos tcp-sequence-past-window
 no ip-mac conflict
 no ip-mac routing conflict
 dhcp-offer-convert
 no stateful-packet-inspection-l2
```

```
!
!
mint-policy global-default
!
meshpoint-qos-policy default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
aaa-policy EXTERNAL-AAA
 authentication server 1 host 192.168.10.6 secret 0 hellomoto
 authentication server 1 proxy-mode through-controller
!
captive-portal LAB-GUEST
 server host captive-portal.tmelabs.local
 server mode centralized-controller hosting-vlan-interface 25
 simultaneous-users 30
 terms-agreement
 webpage internal org-name Motorola Solutions
 webpage internal org-signature &copy 2014 Motorola Solutions. All Rights Reserved.
 use aaa-policy EXTERNAL-AAA
 logout-fqdn logout.tmelabs.local
!
wlan LAB-GUEST
 ssid LAB-GUEST
 vlan 25
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 use captive-portal LAB-GUEST
 captive-portal-enforcement
!
wlan TMELABS-DOT1X
 ssid TMELABS-DOT1X
 vlan 23
 bridging-mode tunnel
 encryption-type ccmp
 authentication-type eap
 wpa-wpa2 exclude-wpa2-tkip
```

```
 use aaa-policy EXTERNAL-AAA
!
wlan TMELABS-PSK
 ssid TMELABS-PSK
 vlan 22
 bridging-mode local
 encryption-type ccmp
 authentication-type none
 wpa-wpa2 psk 0 hellomoto
 wpa-wpa2 exclude-wpa2-tkip
!
ap300 default-ap300
 interface radio1
 interface radio2
!
smart-rf-policy LAB
!
auto-provisioning-policy LAB
 adopt ap6532 precedence 7 profile LAB-AP6532 rf-domain LAB any
!
radius-server-policy INTERNAL-AAA
!
!
management-policy ACCESS-POINTS
 no http server
 ssh
 user admin password 0 hellomoto role superuser access all
 no snmp-server manager v3
!
management-policy CONTROLLERS
 no http server
 https server
 ssh
 user admin password 0 hellomoto role superuser access all
 snmp-server user snmptrap v3 encrypted des auth md5 0 motorola
 snmp-server user snmpoperator v3 encrypted des auth md5 0 motorola
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola
 snmp-server enable traps
 snmp-server host 192.168.10.6 v3 162
!
l2tpv3 policy default
!
```

```
 event-system-policy LAB
  event smrt cov-hole-recovery-done snmp on
  event smrt neighbor-recovery snmp on
  event smrt root-recovery snmp on
  event smrt power-adjustment snmp on
  event smrt calibration-done snmp off
  event smrt config-cleared snmp on
  event smrt channel-change snmp on
  event smrt cov-hole-recovery snmp on
  event smrt interference-recovery snmp on
  event smrt calibration-started snmp off
 !
 profile rfs4000 LAB-RFS4000
  ip name-server 208.67.222.222
  ip name-server 208.67.220.220
  ip domain-name tmelabs.local
  autoinstall configuration
  autoinstall firmware
  crypto ikev1 policy ikev1-default
   isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
   isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  crypto ikev1 remote-vpn
  crypto ikev2 remote-vpn
  crypto auto-ipsec-secure
  crypto remote-vpn-client
  interface radio1
  interface radio2
  interface up1
   description UPLINK
   switchport mode trunk
   switchport trunk native vlan 20
   no switchport trunk native tagged
   switchport trunk allowed vlan 20,23-25
   ip dhcp trust
   qos trust dscp
   qos trust 802.1p
  interface ge1
   ip dhcp trust
   qos trust dscp
   qos trust 802.1p
```

```
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use event-system-policy LAB
 use management-policy CONTROLLERS
 use firewall-policy default
 use auto-provisioning-policy LAB
 use captive-portal server LAB-GUEST
 ntp server 192.168.10.1
 logging on
 no auto-learn-staging-config
 service pm sys-restart
 router ospf
!
profile ap6532 LAB-AP6532
 ip name-server 208.67.222.222
 ip name-server 208.67.220.220
 ip domain-name tmelabs.local
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
```

```
 crypto auto-ipsec-secure
 crypto load-management
 crypto remote-vpn-client
 interface radio1
  wlan TMELABS-DOT1X bss 1 primary
  wlan TMELABS-PSK bss 2 primary
  wlan LAB-GUEST bss 3 primary
 interface radio2
  wlan TMELABS-DOT1X bss 1 primary
 interface ge1
  description UPLINK
  switchport mode trunk
  switchport trunk native vlan 21
  no switchport trunk native tagged
  switchport trunk allowed vlan 21-22
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface vlan21
  description MANAGEMENT
  ip address dhcp
  ip dhcp client request options all
 interface vlan25
  description GUEST
  ip address dhcp
 interface pppoe1
 use management-policy ACCESS-POINTS
 use firewall-policy default
 service pm sys-restart
 router ospf
!
rf-domain LAB
 location "Johnson City TN"
 contact kmarshall@motorolasolutions.com
 timezone EST5EDT
 country-code us
!
rfs4000 00-23-68-22-9D-E4
 use profile LAB-RFS4000
 use rf-domain LAB
 hostname RFS4000-1
 license AP DEFAULT-6AP-LICENSE
```

```
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 ip default-gateway 192.168.20.1
 interface vlan20
  description MANAGEMENT
  ip address 192.168.20.20/24
 cluster name LAB1
 cluster mode active
 cluster member ip 192.168.20.21
 cluster master-priority 254
 logging on
 logging console warnings
 logging buffered warnings
!
rfs4000 5C-0E-8B-1A-E6-D6
 use profile LAB-RFS4000
 use rf-domain LAB
 hostname RFS4000-2
 license AP DEFAULT-6AP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 ip default-gateway 192.168.20.1
 interface vlan20
  description MANAGEMENT
  ip address 192.168.20.21/24
 cluster name LAB1
 cluster mode standby
 cluster member ip 192.168.20.20
 cluster master-priority 128
 logging on
 logging console warnings
 logging buffered warnings
!
ap6532 00-23-68-31-14-2D
 use profile LAB-AP6532
 use rf-domain LAB
 hostname LAB-AP1
!
ap6532 00-23-68-86-44-A0
 use profile LAB-AP6532
 use rf-domain LAB
 hostname LAB-AP2
!
ap6532 5C-0E-8B-A4-48-80
```

```
 use profile LAB-AP6532
 use rf-domain LAB
 hostname LAB-AP3
!
ap6532 5C-0E-8B-A4-4B-48
 use profile LAB-AP6532
 use rf-domain LAB
 hostname LAB-AP4
!
ap6532 5C-0E-8B-A4-4C-3C
 use profile LAB-AP6532
 use rf-domain LAB
 hostname LAB-AP5
!
!
end
```


MOTOROLA SOLUTIONS